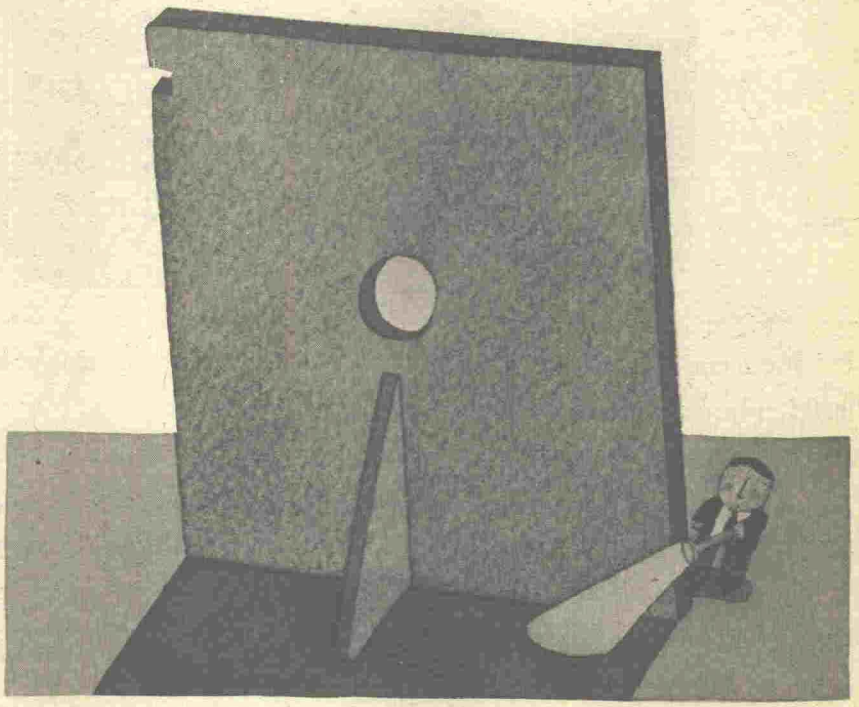
ขจร โรจนเมธินทร์

UNPACKER
หน่วยสนับสนุนการแกะโปรแกรม

โปรแกรมที่ช่วยให้มือดีทั้งหลายแกะหรือดัดแปลงโปรแกรมได้สนุกมือ



ชื่อ UNPACKER เป็นชุดโปรแกรมช่วยเหลือในการแกะโปรแกรมได้ง่ายขึ้น นอกจากนี้ยังมียูทิลิตี้อื่น ๆ ให้เลือกใช้อีก UNPACKER จะเสริมการทำงานของซอฟต์แวร์ SOURCER ในการสร้างซอร์สโค้ดภาษาแอสเซมบลีจากไฟล์ .COM, .EXE หรือไฟล์ไบนารี ทำให้ SOURCER สามารถสร้างซอร์สโค้ดให้มีประสิทธิภาพมากขึ้นในกรณีที่ต้องการสร้างซอร์สโค้ดจากแพคไฟล์ หรือจากไฟล์แบบ multi-segment COM

UNPACKER ทำงานกับดอสรุ่น 2.0 ขึ้นไป โดยต้องมีหน่วยความจำไม่ต่ำกว่า 384K จอภาพที่ใช้งานอาจเป็นทั้งเอ็มดีเอ, ซีจีเอ, อีจีเอ, วีจีเอ และเฮอร์คิวลิส

ส่วนประกอบของ UNPACKER

ชุดของ UNPACKER ประกอบด้วย 4 โปรแกรมรวมอยู่บนดิสก์แผ่นเดียว คือ

1. UNPACK เป็นโปรแกรมที่จะแปลงไฟล์ packed EXE ให้กลายเป็นไฟล์ unpacked EXE และทำการค้นหาส่วนโอเวอร์เลย์ ซึ่งสามารถให้โปรแกรม UNPACK แยกออกมาจากส่วนโปรแกรมหลัก

2. COM2EXE ทำหน้าที่ค้นหาและแปลงไฟล์ multi-segment COM ให้กลายเป็นไฟล์ EXE

3. INTVIEW จะแสดงรายละเอียดของตารางอินเตอร์รัพต์ทั้ง 256 อินเตอร์รัพต์

4. VTEST จะแก้ไขโหมดของจอภาพ เพจของจอภาพ และทำการทดสอบจอภาพ นอกจากนี้ยังช่วยในการดีบัก การทำงานของ TSR ที่เกี่ยวกับจอภาพ

UNPACK

การใช้งาน UNPACK เรียกจากดอสพรอมต์โดย

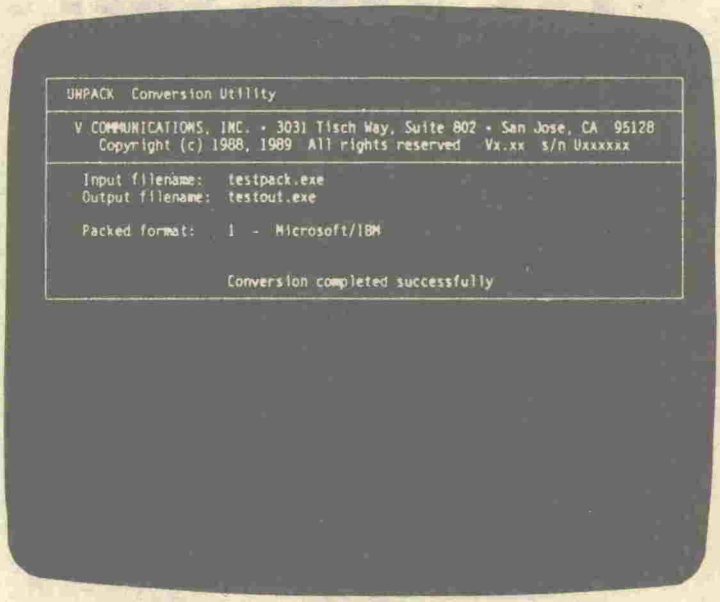
```
C:> unpack filename1 filename2
```

filename 1 คือไฟล์ packed ที่เราจะแปลง หากไม่ใส่นามสกุล UNPACK จะใช้ .EXE

filename 2 คือไฟล์ unpacked ที่ UNPACK จะสร้างขึ้นมา

จากรูปที่ 1 UNPACK จะทำการแปลง testpack.exe ซึ่งเป็นไฟล์ packed ให้เป็นไฟล์ unpacked แล้วเขียนลงใน testout.exe สำหรับฟอร์แมตของไฟล์ packed ในตัวอย่างนี้คือ Microsoft/IBM

หลังจากการแปลงในเฟสแรกเสร็จ



รูปที่ 1
แสดงจอภาพหลังจากที่รัน UNPACK

เรียบร้อย unpacked จะตรวจสอบส่วนโอเวอร์เลย์ให้ ถ้าค้นพบจะแสดงข้อความ

```
Appended overlays detected. Append to make a runable copy (Yes/No)?
```

ถ้าเราต้องการให้ไฟล์ unpacked ที่ได้สามารถรันหรือใช้สำหรับดีบักเกอร์ก็ตอบ 'Y' แต่ถ้าต้องการใช้ SOURCER สร้างซอร์สโค้ดให้ตอบ 'N' เพื่อที่ UNPACK จะได้แยกเอาส่วนโอเวอร์เลย์ออกจากโปรแกรมหลัก จากนั้น UNPACK จะถามคำถามที่สองว่า

```
Do you wish to write overlays to individual files (Yes/No)?
```

ถ้าตอบ 'N' โปรแกรม UNPACK จะตัดส่วนโอเวอร์เลย์ออกจากโปรแกรมหลัก แต่ถ้าตอบ 'Y' เราจะต้องใส่ชื่อไฟล์สำหรับส่วนโอเวอร์เลย์ที่ UNPACK จะสร้างดังนี้

```
Enter filename for overlays :
```

สำหรับชื่อไฟล์นั้นเราจะตั้งชื่อได้ 6 คาแรคเตอร์ โดยอีก 2 คาแรคเตอร์จะกันไว้ใส่ตัวเลข 01-99 เพราะฉะนั้น UNPACK จะสร้างไฟล์แบบโอเวอร์เลย์ได้ถึง 99 ไฟล์

ถ้า UNPACK ไม่สามารถค้นพบการ pack จะหมายถึงจบการทำงาน หรืออาจพบส่วนโอเวอร์เลย์อย่างเดียวก็ได้ UNPACK จะถามว่า

```
Appended overlays detected. Write to individual files (Yes/No)?
```

ถ้าตอบ 'Y' ก็จะมีการสร้างไฟล์แบบโอเวอร์เลย์ให้

COM2EXE

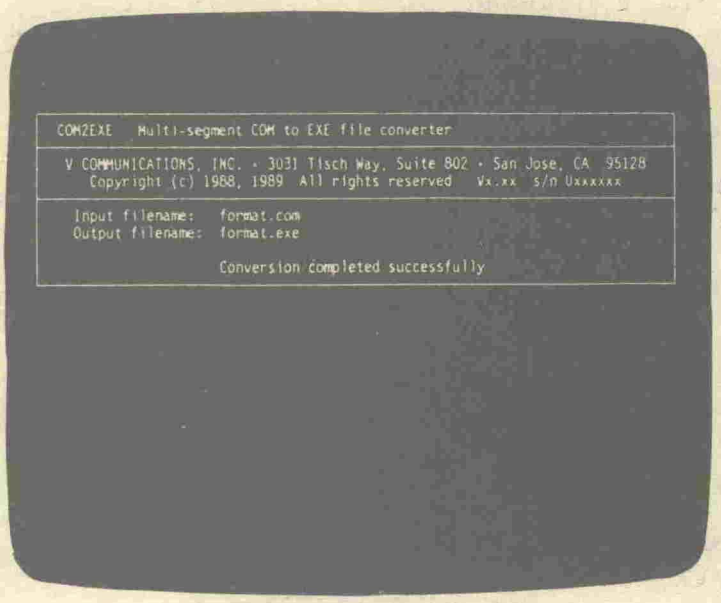
โปรแกรมของดอสจากไอบีเอ็มและไมโครซอฟต์บางส่วนจะเป็นฟอร์แมตแบบ multi-segment COM ซึ่งความจริงแล้วฟอร์แมตนี้ไม่มีผลในการรันโปรแกรม แต่หลังจากแปลงให้เป็นฟอร์แมต EXE ด้วย COM2EXE แล้ว จะทำให้การโหลดและรันโปรแกรมเร็วขึ้น

การเรียกใช้ COM2EXE ทำได้ดังนี้

```
C: > com2exe filename
```

filename จะเป็นชื่อไฟล์ที่มีฟอร์แมตแบบ multi-segment COM ถ้าเราไม่ใส่นามสกุล COM2EXE จะใช้นามสกุลแบบ COM โดยอัตโนมัติ แล้ว COM2EXE จะสร้างไฟล์ฟอร์แมต EXE ให้

หลังจากรัน COM2EXE แล้วจอภาพจะแสดงดังรูปที่ 2 และถ้าอินพุตไฟล์ไม่เป็น multiple-segment จะไม่มีการสร้างไฟล์ใดเกิดขึ้น สำหรับไฟล์ที่ COM2EXE สร้างขึ้นจะเป็นแบบ EXE ซึ่งสามารถใช้ SOURCER ต่อไปได้ ดังตารางที่ 1



รูปที่ 2
แสดงหน้าจอหลังจากรัน COM2EXE

ไฟล์	MS-DOS 2.00	PC-DOS 3.00	MS-DOS 3.30	PC-DOS 4.00
BACKUP.COM	no	no	no	YES
CHKDSK.COM	no	YES	YES	YES
DEBUG.COM	no	YES	YES	YES
EDLIN.COM	no	YES	YES	YES
FDISK.COM	no	no	YES	no
FORMAT.COM	no	YES	YES	YES
GRAFTABL.COM	n/a	no	YES	no
GRAPHICS.COM	no	no	YES	no
PRINT.COM	no	YES	YES	YES
RECOVER.COM	no	YES	YES	YES
RESTORE.COM	no	no	no	YES
SYS.COM	no	YES	YES	no

(n/a หมายถึงยังไม่มีโปรแกรมนี้ใช้)

ตารางที่ 1 แสดงรายชื่อไฟล์ของดอสที่เป็นฟอร์แมตแบบ multi-segment COM

INTVIEW

เมื่อเรารัน INTVIEW จากดอสพรอมต์ INTVIEW จะแสดงรายละเอียดของอินเตอร์รัพต์ 16 หมายเลขแรก ดังรูปที่ 3

คอลัมน์แรก Int จะแสดงหมายเลขของอินเตอร์รัพต์จาก 00h-FFh

คอลัมน์ที่สอง seg:off แสดงเซกเมนต์และออฟเซตที่อินเตอร์รัพต์นั้นชี้ไป

คอลัมน์ที่สาม Comments แสดงรายละเอียดของบริเวณที่อินเตอร์รัพต์ชี้ไป โดยค้นหาสตริงของข้อความ เช่น "Copyright (C) 1989"

คอลัมน์ที่สี่ Function จะอธิบายหน้าที่ของอินเตอร์รัพต์อย่างคร่าว ๆ

คำสั่งของ INTVIEW

PgUp = แสดงหน้าถัดไป อาจใช้สเปซบาร์ก็ได้

PgDn = แสดงหน้าก่อนหน้า

Space = แสดงหน้าถัดไป

S = เก็บรายละเอียดทั้งหมดลงในไฟล์ชื่อ INTVIEW.OUT

Esc = ออกไปสู่ดอส

0-F=เลือกกลุ่มของอินเตอร์รัพต์ให้แสดงบนจอภาพ

VTEST

VTEST เป็นโปรแกรมตัวหนึ่งในชุดของ UNPACKER ซึ่งจะช่วยทดสอบวิดีโออะแดปเตอร์ และทดสอบการทำงานของโปรแกรมประเภท TSR ในส่วนที่เกี่ยวกับจอภาพ หลังจากที่เรารัน VTEST หน้าจอจะปรากฏดังรูปที่ 4

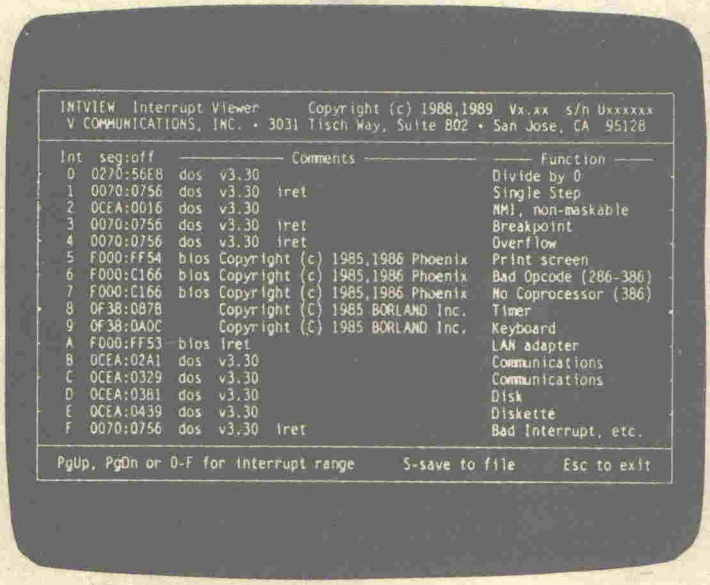
การใช้งาน VTEST เริ่มด้วยการเลือกโหมดของจอภาพก่อน โดยใส่หมายเลข 00h-FFh จากนั้นก็ใช้คำสั่งต่อไปนี้

PgUp = เขียนแพตเทอร์นของการทดสอบบนหน้าถัดไป

PgDn = เขียนแพตเทอร์นของการทดสอบบนหน้าก่อนหน้า

Up Arrow = ไปหน้าถัดไปโดยไม่มีการเขียนแพตเทอร์นในการทดสอบ

รูปที่ 3
แสดงหน้าจอหลังจากรัน INTVIEW



Down Arrow = กลับไปหน้าก่อนหน้าโดยไม่มีการเขียนแพตเทอร์นในการทดสอบ

H = เลือกโหมดโมโนโครมของเฮอร์คิวลิส โดยต้องเลือกโหมด 7 ก่อน

L = เปลี่ยนเป็นโหมด 43 บรรทัด ใช้ได้กับอีจีเอและวีจีเอเท่านั้น

M = กลับไปโหมดเดิม และแสดงเมนูของ VTEST

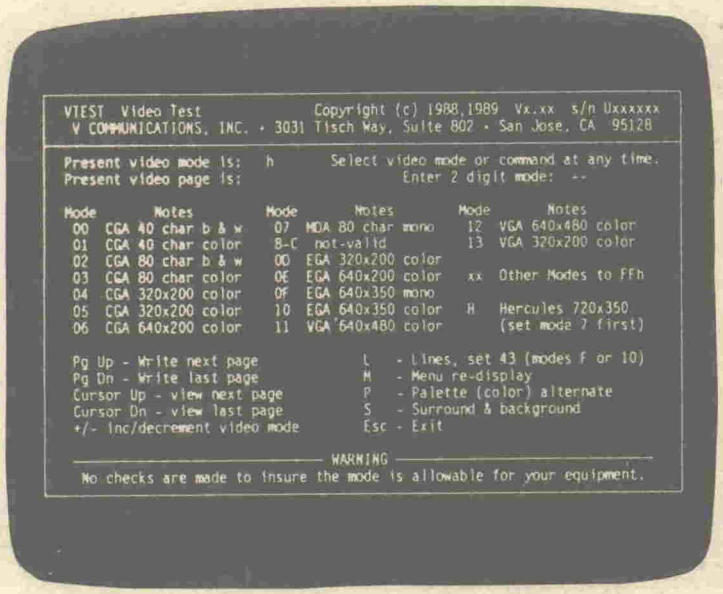
P = เปลี่ยนจากพาเลตต์หนึ่งไปอีกกลุ่มหนึ่ง

S = เปลี่ยนสีขอบและแบคกราวนด์

\+ = ไปยังโหมดถัดไป

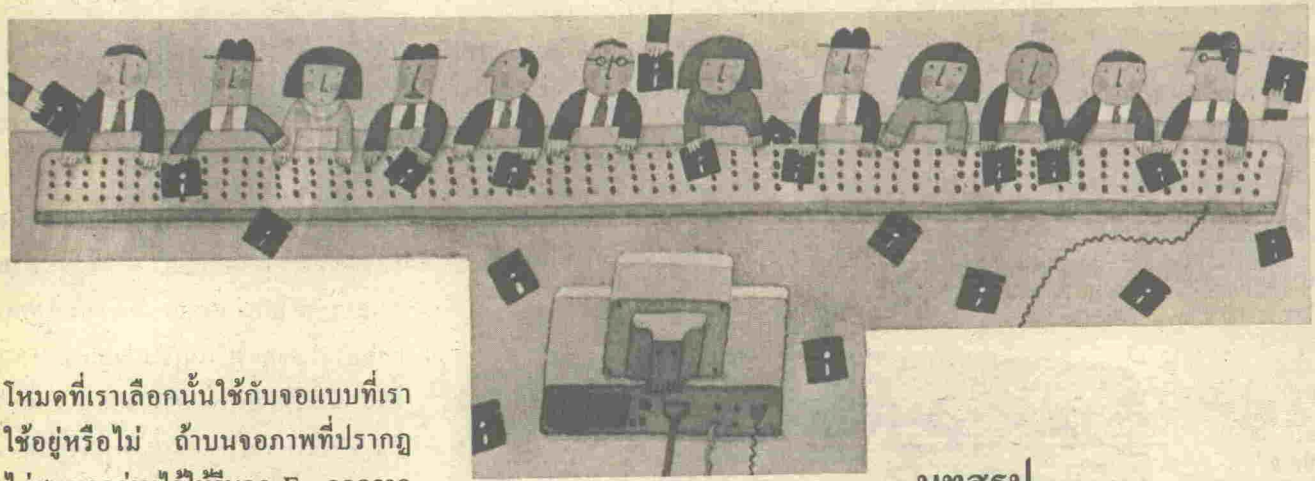
− = ไปยังโหมดก่อนหน้า

Esc = กลับไปยังดอส



รูปที่ 4 แสดงจอภาพหลังจากรัน VTEST

ข้อควรระวังสำหรับการใช้ VTEST ก็คือ โปรแกรมจะไม่ทำการตรวจสอบว่าโหมดที่เราเลือกนั้นใช้กับจอแบบที่เราใช้อยู่หรือไม่ ถ้าบนจอภาพที่ปรากฏไม่สามารถอ่านได้ให้รีบกด Esc ออกจาก VTEST ทันที มิฉะนั้นอาจจะเกิดความเสียหายขึ้นกับจอภาพได้ เนื่องจากจอภาพถูกบังคับให้ทำงานเกินกว่าที่ผู้ผลิตกำหนด จอภาพอาจไหม้ได้



ทดสอบโปรแกรม TSR โดย VTEST

เราสามารถใช้ VTEST ทดสอบการทำงานของโปรแกรมประเภท TSR ว่าทำงานได้ถูกต้องกับจอภาพประเภทต่าง ๆ หรือไม่ เนื่องจากโปรแกรมประเภท TSR บางโปรแกรมไม่สามารถทำงานกับจอภาพได้ทุกประเภท ดังนั้นจึงอาจเกิดความเสียหายกับจอภาพ

วิธีการทดสอบด้วย VTEST เราจะต้องโหลดโปรแกรม TSR ลงบนหน่วยความจำก่อน ต่อจากนั้นก็รัน VTEST และเลือกโหมดจอภาพ โดยเริ่มจากโหมด 0 แล้วป๊อปอัพโปรแกรม TSR ขึ้นมา และออกจากโปรแกรม TSR จอภาพควรจะไม่เปลี่ยนไปหลังจากเรียกโปรแกรม TSR คือจอภาพยังคงเป็นเมนูของ VTEST แสดงว่าการทำงานของโปรแกรม TSR สำหรับจอภาพโหมดนั้นทำได้

บทสรุป

UNPACKER เป็นชุดโปรแกรมที่สนับสนุนการทำงานของ SOURCER ให้ทำงานได้มีประสิทธิภาพสูงขึ้นคือ UNPACK และ COM2EXE นอกจากนี้ยังมียูทิลิตี้อื่นคือ INTVIEW และ VTEST ลองหาซอฟต์แวร์ตัวนี้มาลองใช้กันเองนะครับ รับรองว่าจะติดใจ